FIG.1

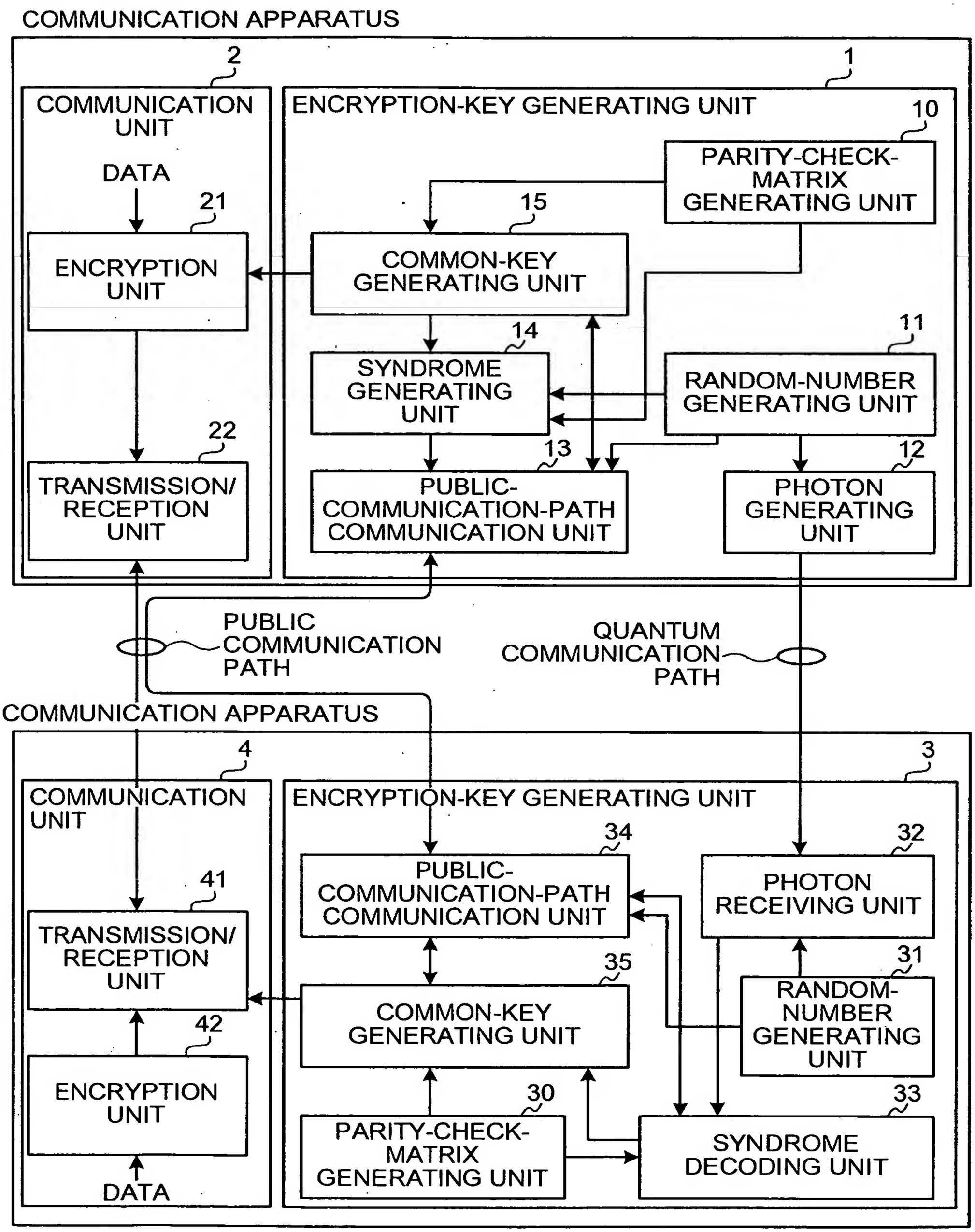

COMMUNICATION APPARATUS
2
COMMUNICATION UNIT
DATA
21
ENCRYPTION UNIT
22
TRANSMISSION/ RECEPTION UNIT
1
ENCRYPTION-KEY GENERATING UNIT
10
PARITY-CHECK-MATRIX GENERATING UNIT
15
COMMON-KEY GENERATING UNIT
14
SYNDROME GENERATING UNIT
11
RANDOM-NUMBER GENERATING UNIT
13
PUBLIC-COMMUNICATION-PATH COMMUNICATION UNIT
12
PHOTON GENERATING UNIT
PUBLIC COMMUNICATION PATH
QUANTUM COMMUNICATION PATH
COMMUNICATION APPARATUS
4
COMMUNICATION UNIT
41
TRANSMISSION/ RECEPTION UNIT
42
ENCRYPTION UNIT
DATA
3
ENCRYPTION-KEY GENERATING UNIT
34
PUBLIC-COMMUNICATION-PATH COMMUNICATION UNIT
32
PHOTON RECEIVING UNIT
35
COMMON-KEY GENERATING UNIT
31
RANDOM-NUMBER GENERATING UNIT
30
PARITY-CHECK-MATRIX GENERATING UNIT
33
SYNDROME DECODING UNIT

FIG.2

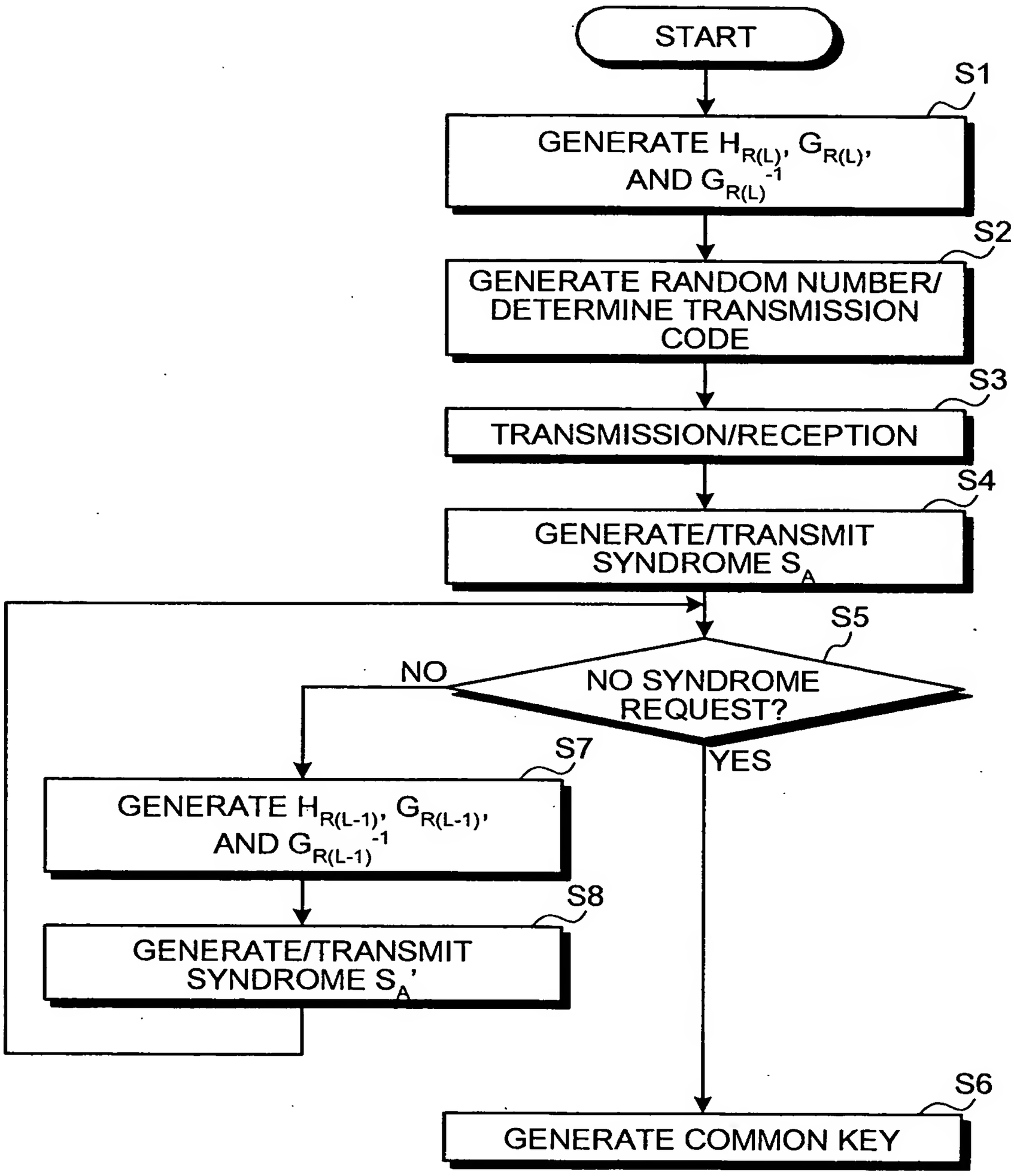

START
S1
GENERATE $H_{R(L)}$, $G_{R(L)}$, AND $G_{R(L)}^{-1}$
S2
GENERATE RANDOM NUMBER/ DETERMINE TRANSMISSION CODE
S3
TRANSMISSION/RECEPTION
S4
GENERATE/TRANSMIT SYNDROME S_A
S5
NO SYNDROME REQUEST?
NO
YES
S7
GENERATE $H_{R(L-1)}$, $G_{R(L-1)}$, AND $G_{R(L-1)}^{-1}$
S8
GENERATE/TRANSMIT SYNDROME S_A'
S6
GENERATE COMMON KEY

FIG.3

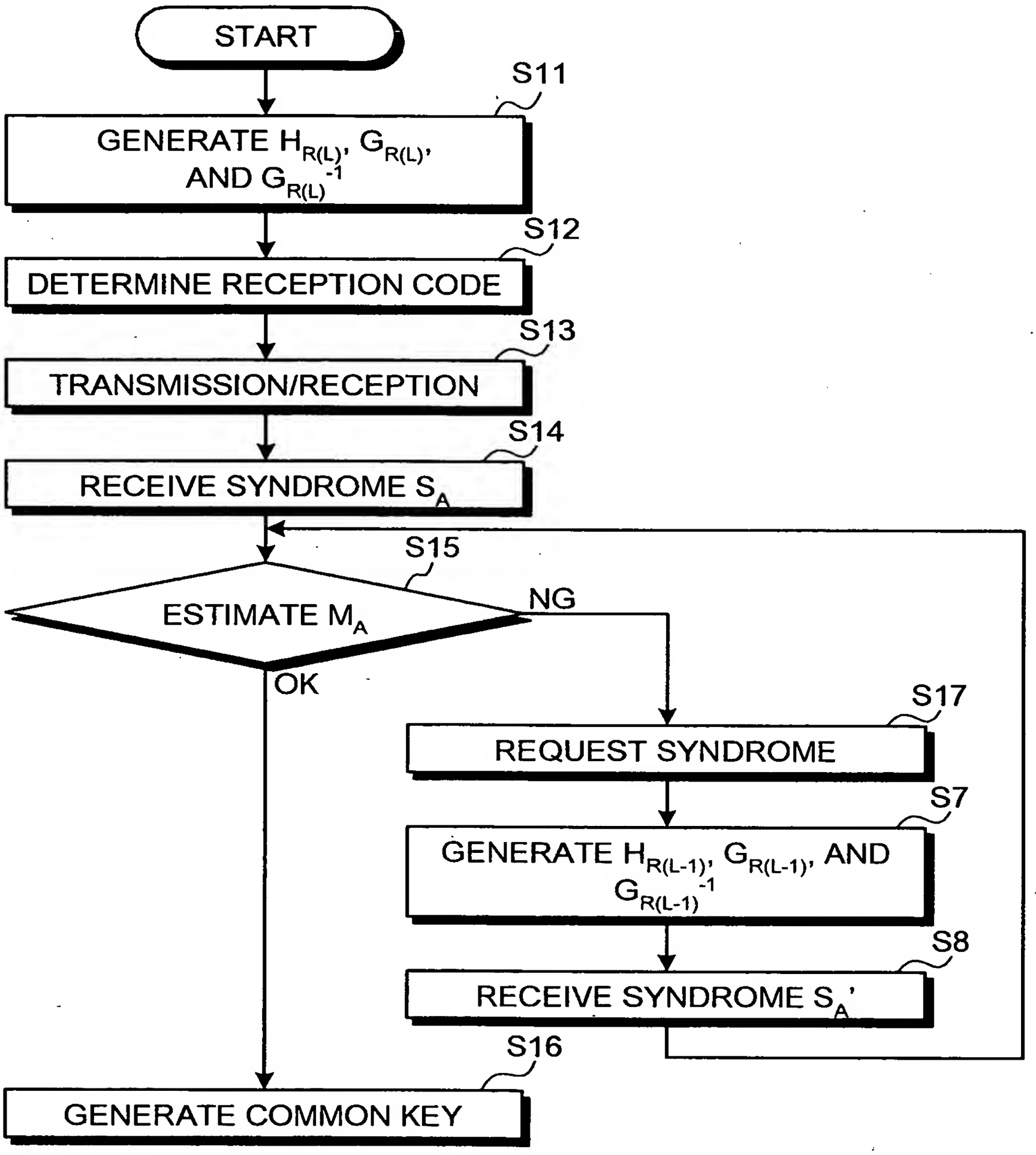

START
S11
GENERATE $H_{R(L)}$, $G_{R(L)}$, AND $G_{R(L)}^{-1}$
S12
DETERMINE RECEPTION CODE
S13
TRANSMISSION/RECEPTION
S14
RECEIVE SYNDROME S_A
S15
ESTIMATE M_A
NG
OK
S17
REQUEST SYNDROME
S7
GENERATE $H_{R(L-1)}$, $G_{R(L-1)}$, AND $G_{R(L-1)}^{-1}$
S8
RECEIVE SYNDROME S_A'
S16
GENERATE COMMON KEY

FIG.4

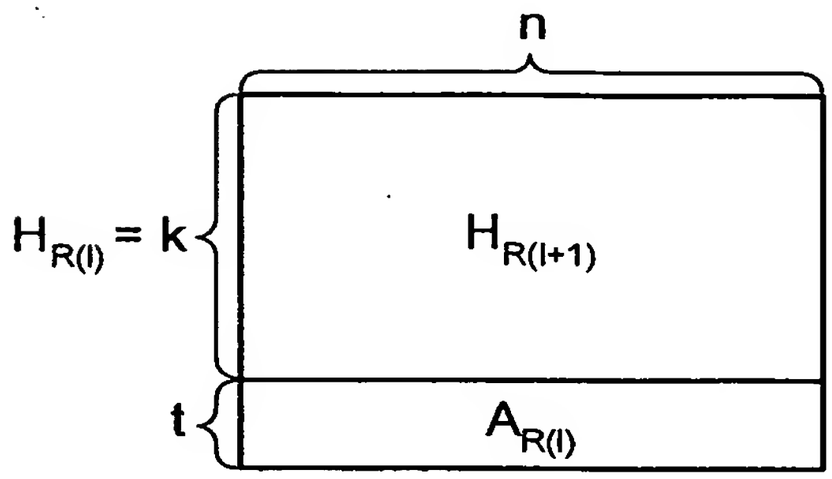

n
$H_{R(l)}$ = k
$H_{R(l+1)}$
t
$A_{R(l)}$

FIG.5

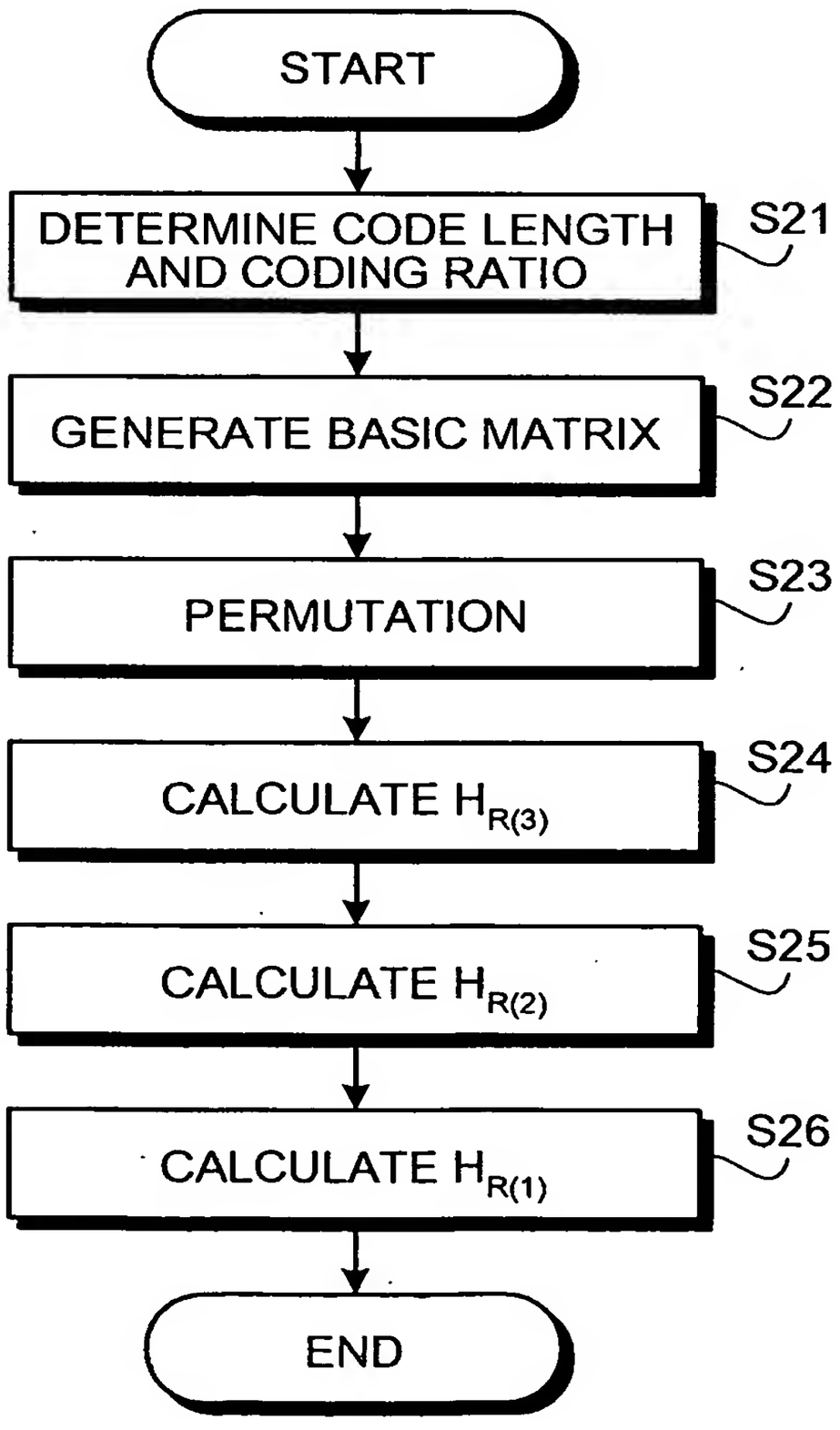

START
DETERMINE CODE LENGTH AND CODING RATIO
S21
GENERATE BASIC MATRIX
S22
PERMUTATION
S23
CALCULATE $H_{R(3)}$
S24
CALCULATE $H_{R(2)}$
S25
CALCULATE $H_{R(1)}$
S26
END

FIG.6

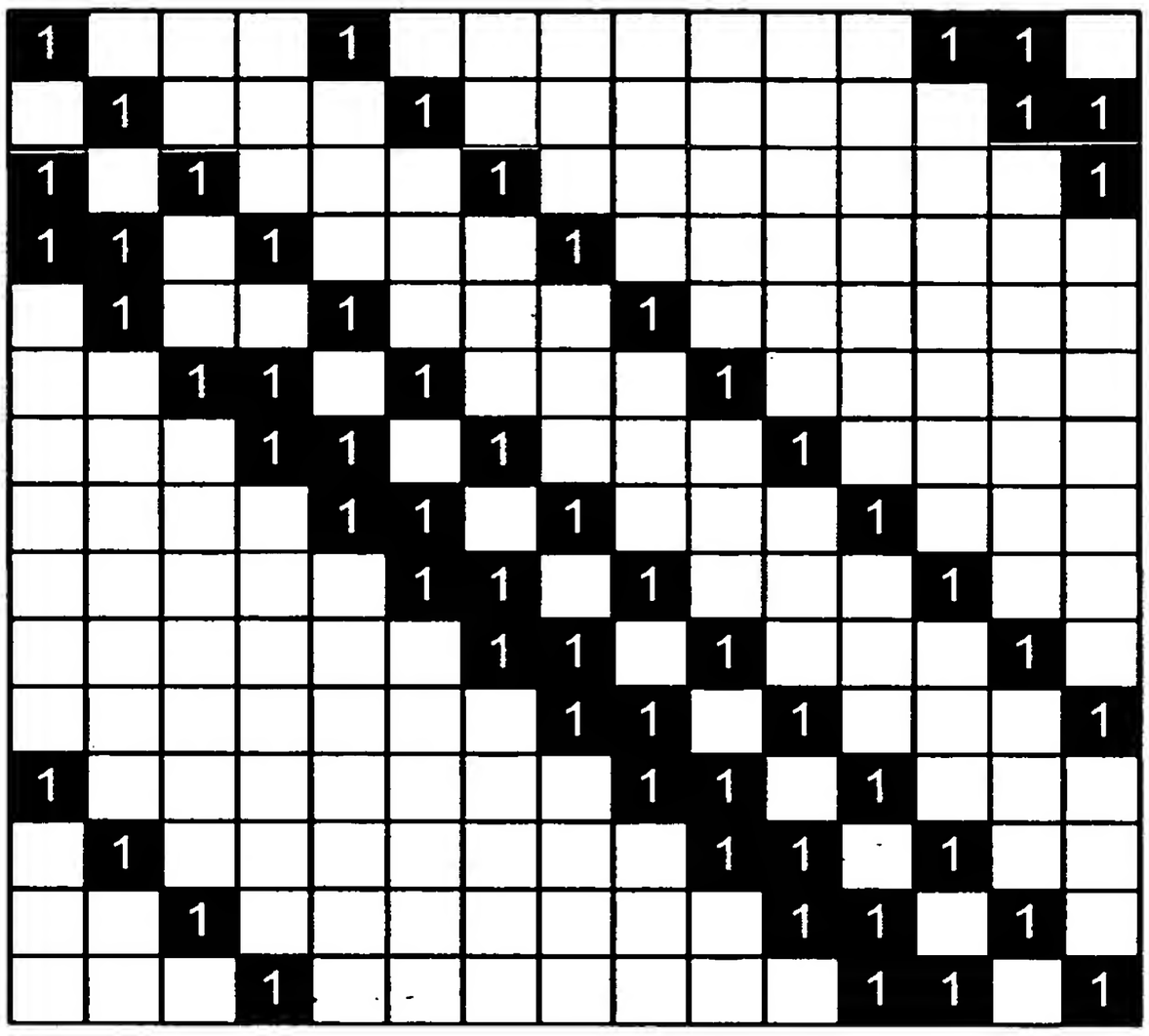


FIG.7

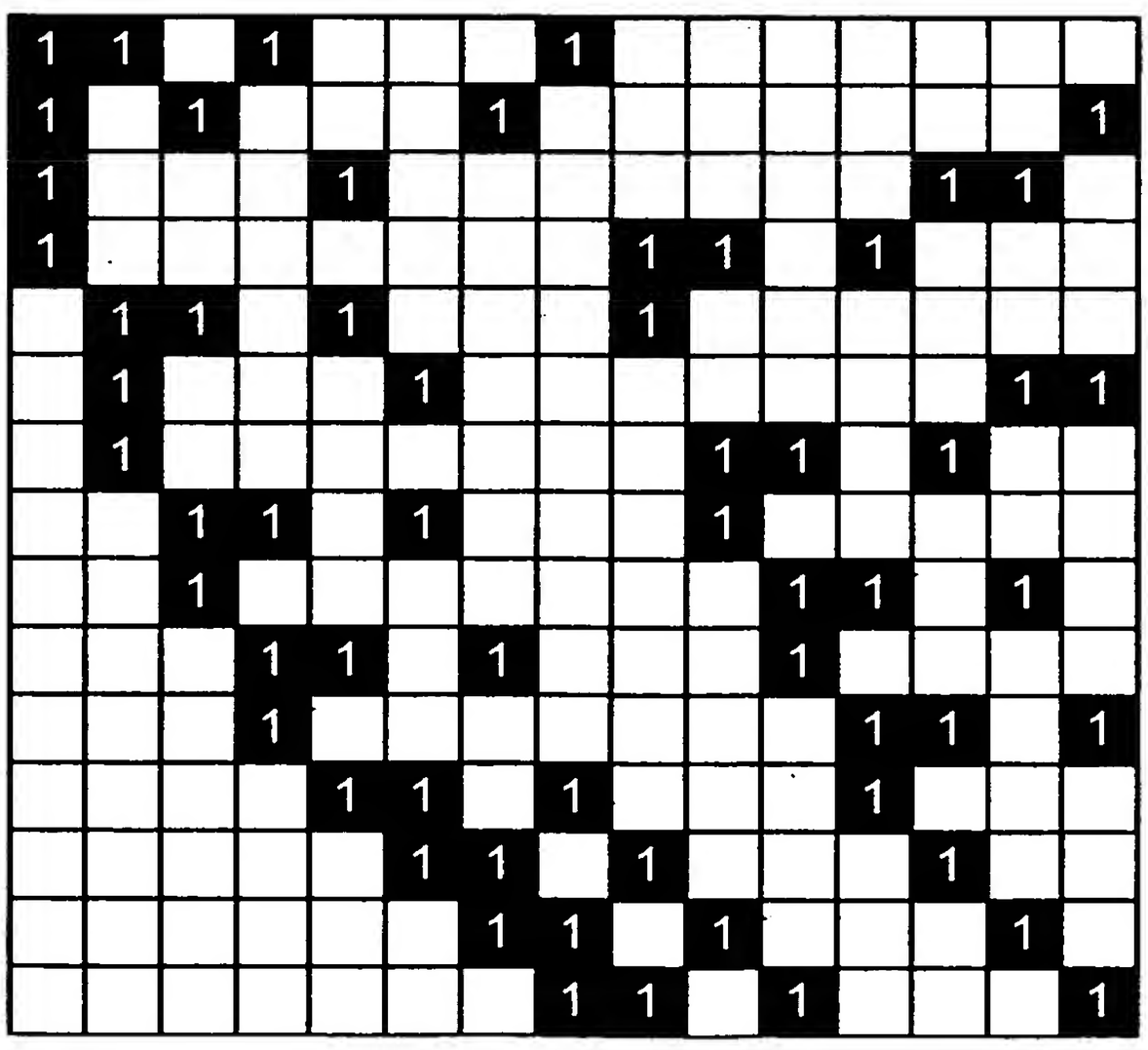


FIG.8

RATE	RATE=0.6
ORDER i	COLUMN ORDER RATIO $\lambda_i(R(I))$
1	
2	0.01
3	0.970022733
4	0.019977267
ORDER i	ROW ORDER RATIO $\rho_i(R(I))$
2	
7	7/15
8	8/15

FIG.9

$H_{R(l)=0.6}$

ORDER i	COLUMN ORDER RATIO $\lambda_i(R(l))$	NUMBER OF COLUMNS $n_v(x,R(l))(m'=1000)$
1	0.0372	279
2	0.8884	4442
3	0.0744	279

ORDER i	ROW ORDER RATIO $\rho_i(R(l))$	NUMBER OF ROWS $n_c(x,R(l))(m'=1000)$
2	7/15	1000
3	8/15	1000
7		
8		

FIG.10

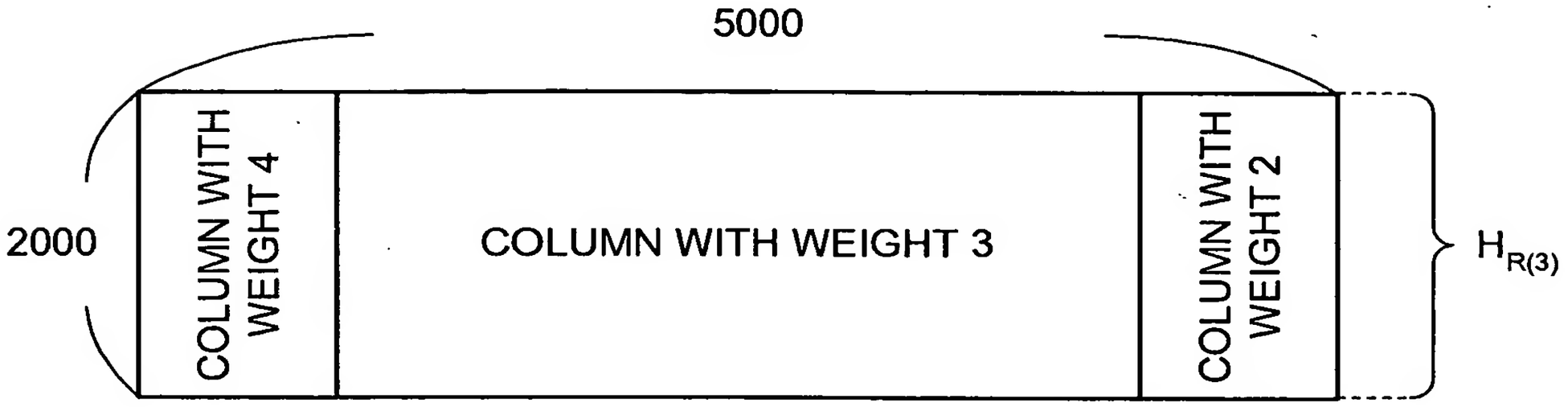

5000
2000
COLUMN WITH WEIGHT 4
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
$H_{R(3)}$

FIG.11

	$H_{R(l)=0.6}$		$H_{R(l-1)=0.4}$		$A_{R(l-1)=0.4}$
ORDER i	COLUMN ORDER RATIO $\lambda_i(R(l))$	NUMBER OF COLUMNS $n_v(x,R(l))$ (m'=1000)	COLUMN ORDER RATIO $\lambda_i(R(l-1))$	NUMBER OF COLUMNS $n_v(x,R(l-1))$ (m'=1000)	NUMBER OF COLUMNS
1					150 COLUMN IDENTICAL WITH $\lambda_3(R(l))$: 150
2	0.0372	279	0.0310	279	6 COLUMN IDENTICAL WITH $\lambda_3(R(l))$: 6
3	0.8884	4442	0.6133	3619	946 COLUMN IDENTICAL WITH $\lambda_4(R(l))$: 279 COLUMN IDENTICAL WITH $\lambda_3(R(l))$: 667
4	0.0744	279	0.0333	150	
5			0.0017	6	
6			0.2833	667	
7			0.0373	279	
ORDER i	ROW ORDER RATIO $\rho_i(R(l))$	NUMBER OF ROWS $n_c(x,R(l))$ (m'=1000)	ROW ORDER RATIO $\rho_i(R(l-1))$	NUMBER OF ROWS $n_c(x,R(l-1))$ (m'=1000)	
2					
3			3/18	1000	
7	7/15	1000	7/18	1000	
8	8/15	1000	8/18	1000	

App No.: NEW
Inventor: Wataru MATSUMOTO
Title: QUANTUM KEY DISTRIBUTION METHOD AND COMMUNICATION APPARATUS
NEW SHEET
Docket No.: 2611-0260PUS1
Sheet 9 of 13

FIG.12

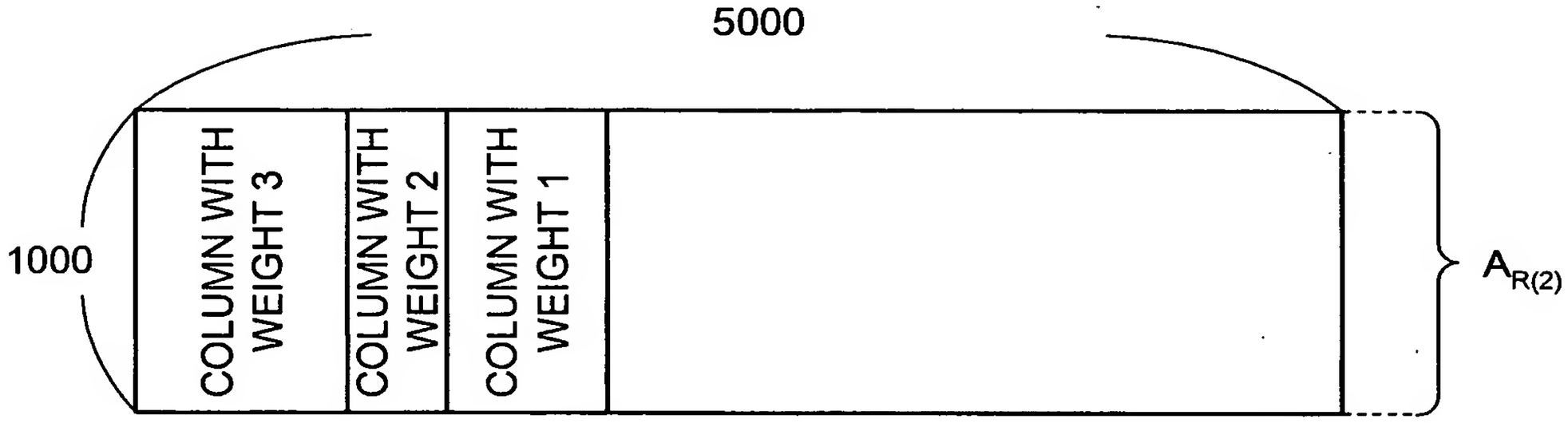

5000
1000
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
COLUMN WITH WEIGHT 1
$A_{R(2)}$

FIG.13

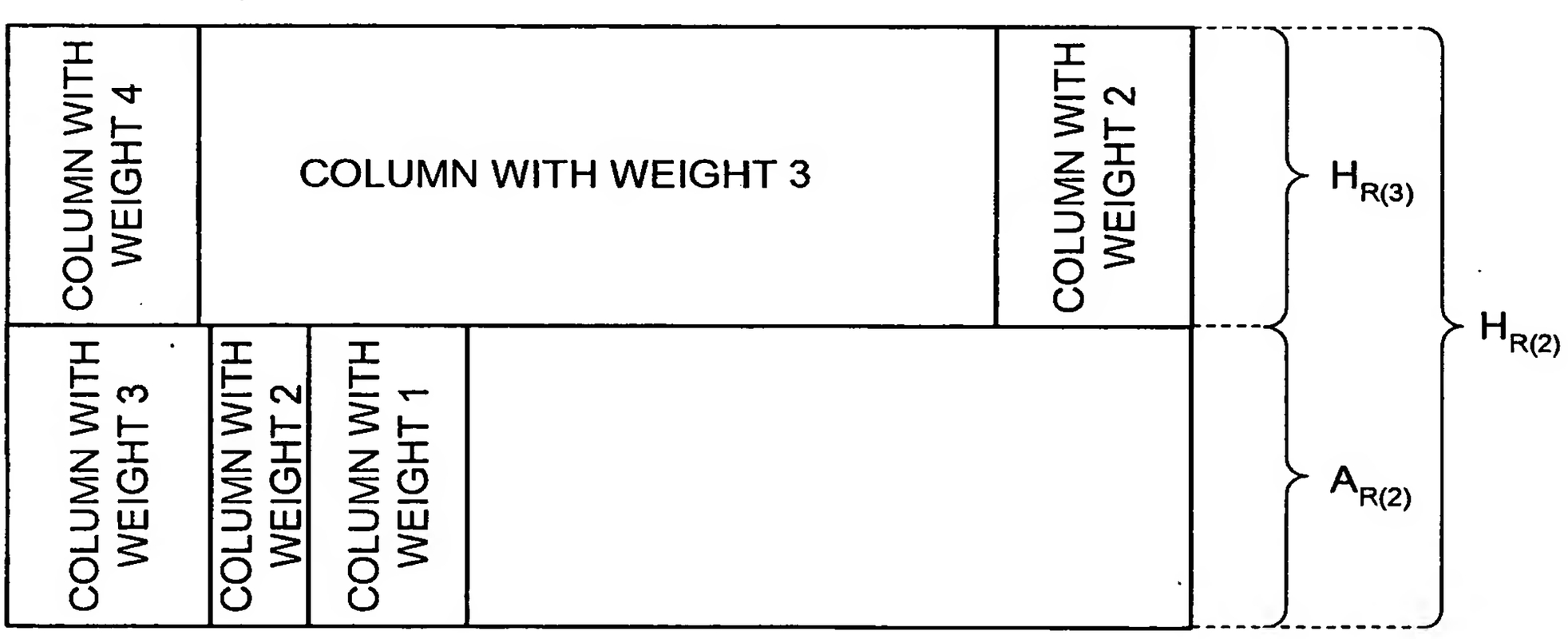

COLUMN WITH WEIGHT 4
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
COLUMN WITH WEIGHT 1
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
COLUMN WITH WEIGHT 1
$H_{R(3)}$
$A_{R(2)}$
$H_{R(2)}$

FIG.14

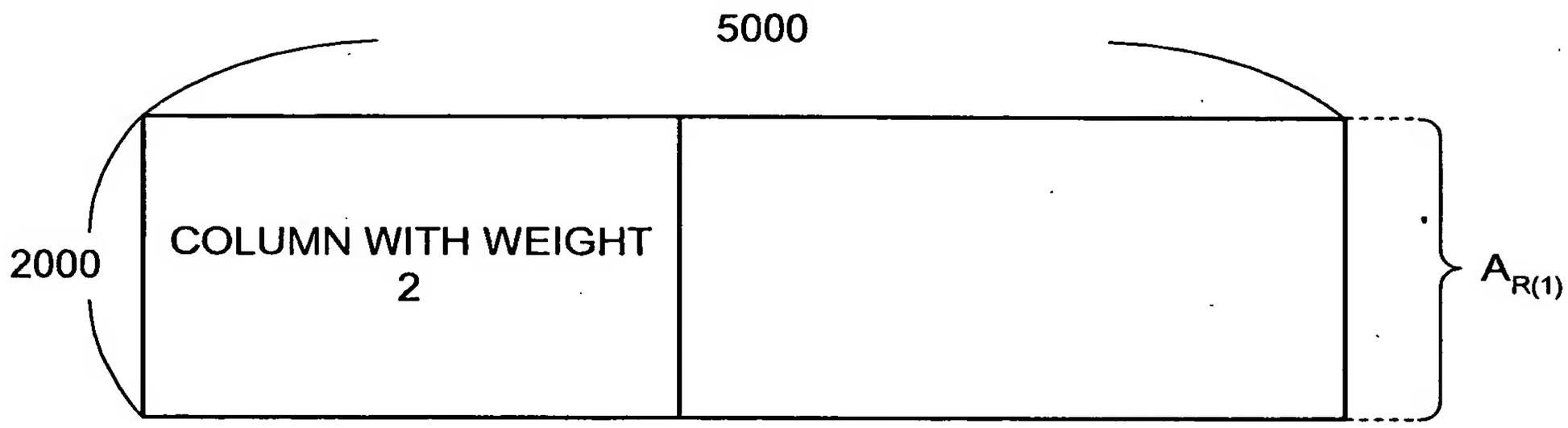

5000
2000
COLUMN WITH WEIGHT 2
$A_{R(1)}$

FIG.15

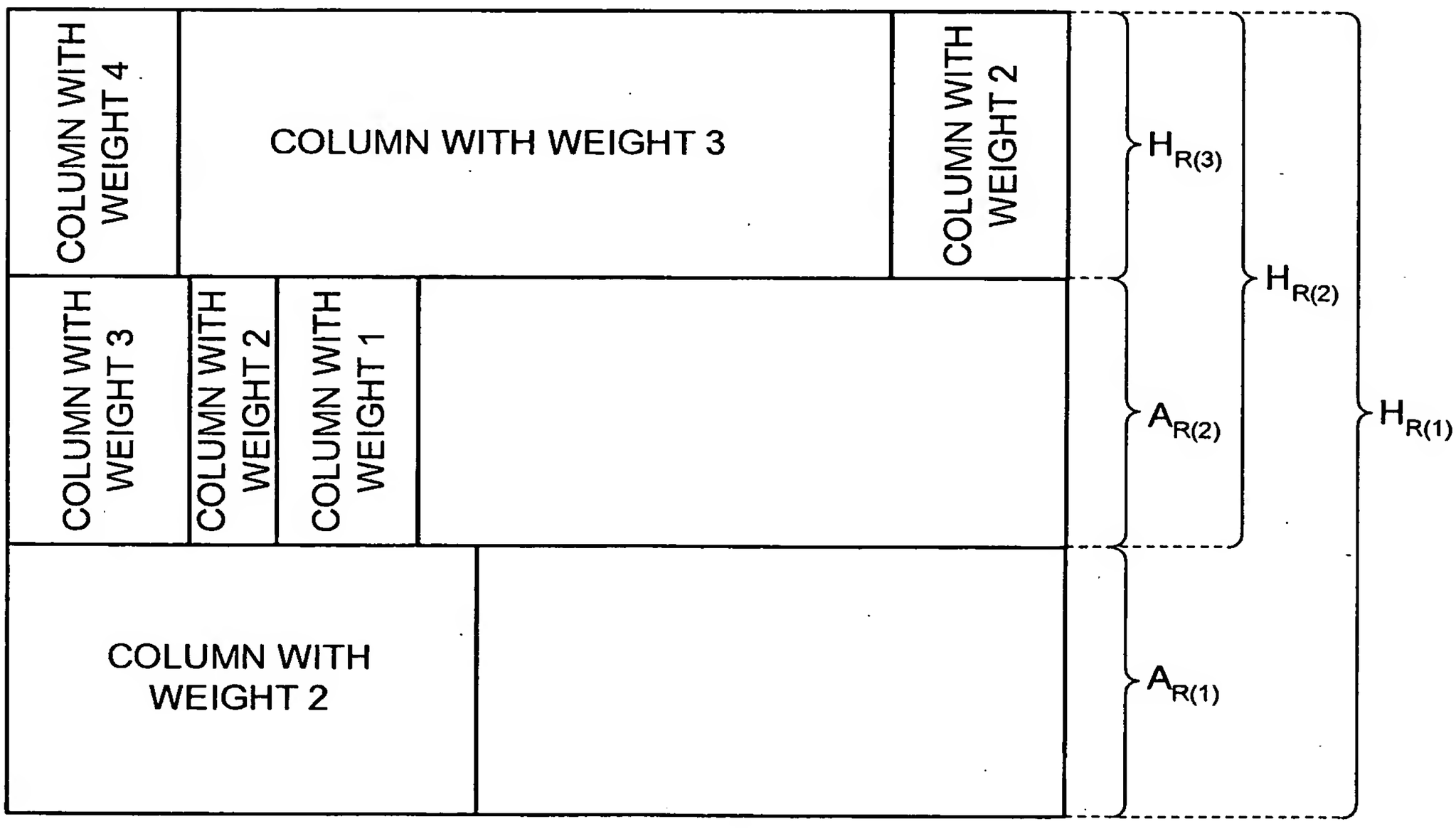

COLUMN WITH WEIGHT 4
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
COLUMN WITH WEIGHT 3
COLUMN WITH WEIGHT 2
COLUMN WITH WEIGHT 1
COLUMN WITH WEIGHT 2
$H_{R(3)}$
$H_{R(2)}$
$H_{R(1)}$
$A_{R(2)}$
$A_{R(1)}$

FIG.16

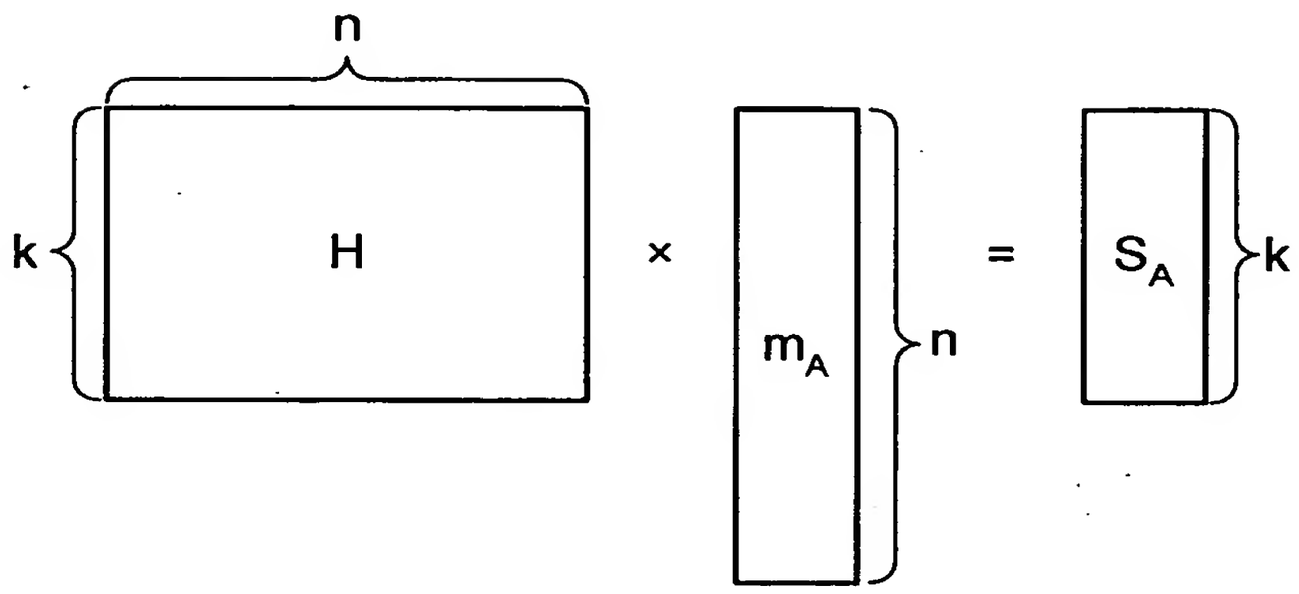


FIG.17

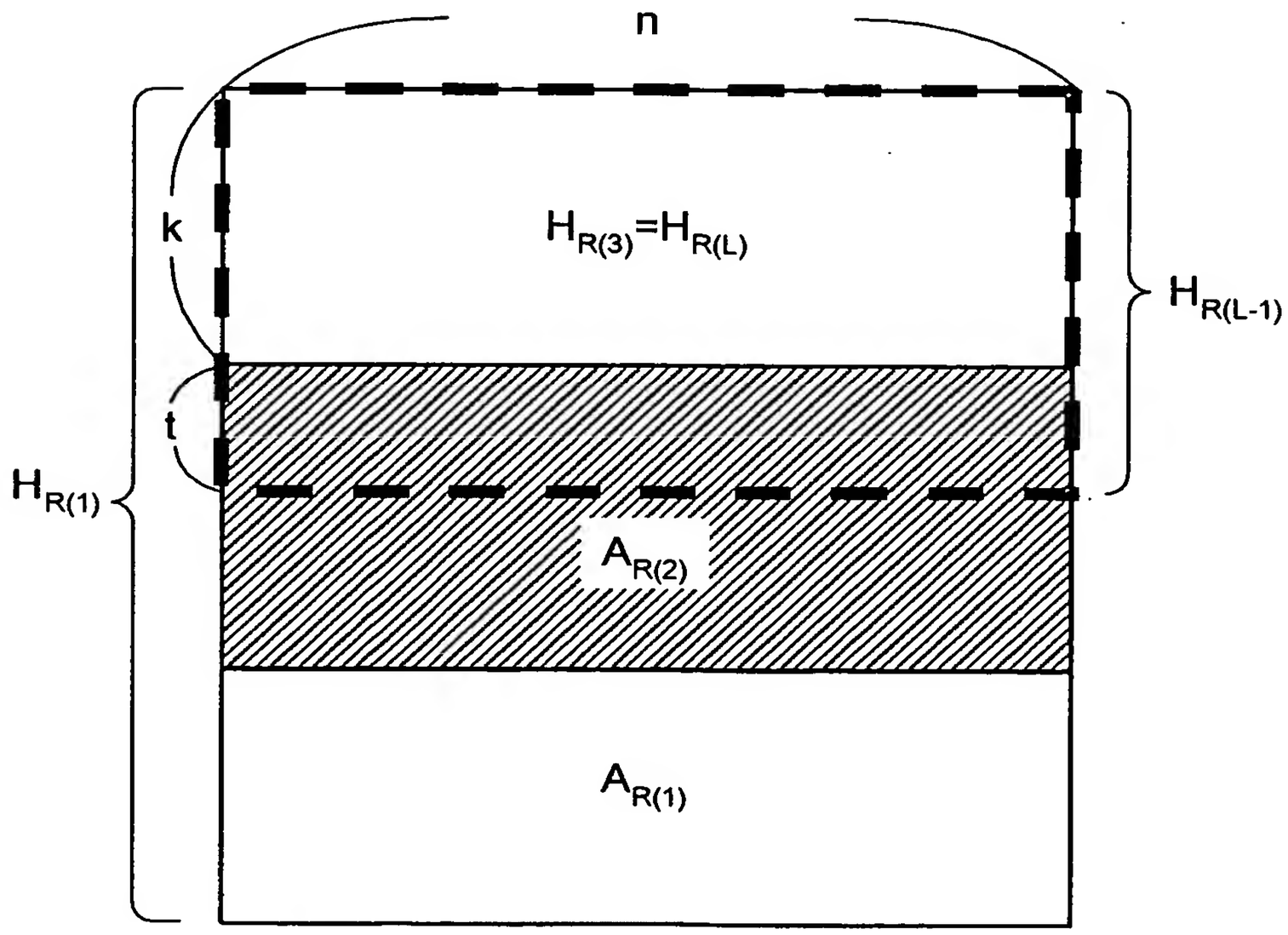


FIG.18

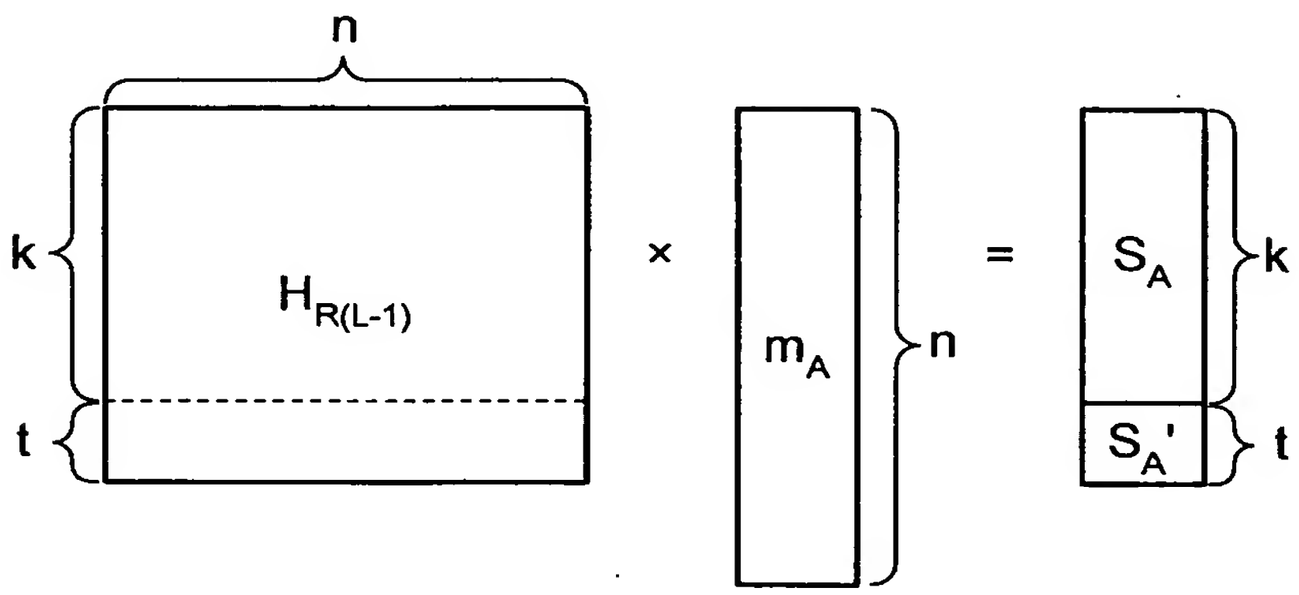
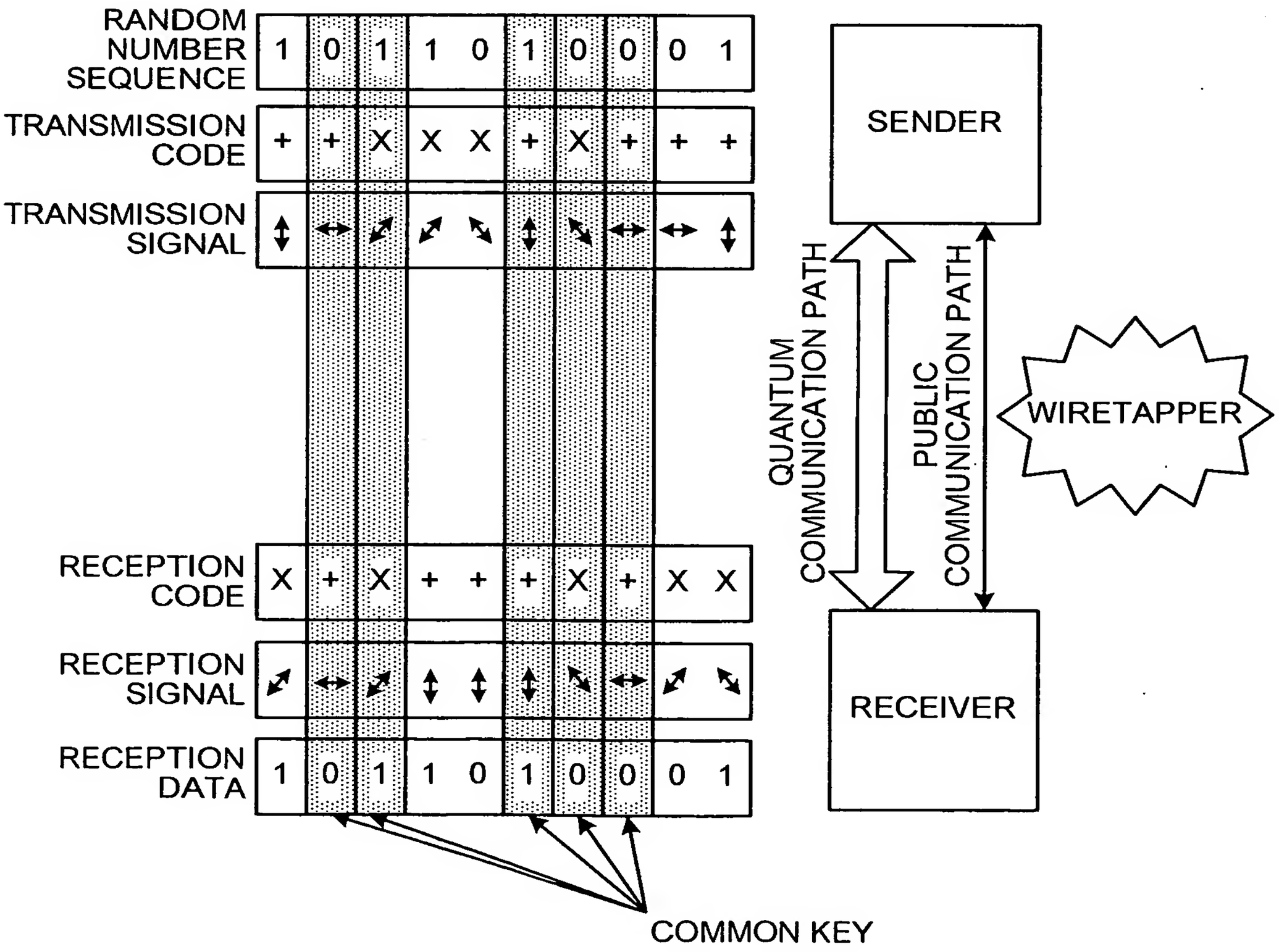

n
k
t
$H_{R(L-1)}$
×
m_A
n
=
S_A
k
S_A'
t

FIG.19


RANDOM NUMBER SEQUENCE
1 0 1 1 0 1 0 0 0 1
TRANSMISSION CODE
+ + X X X + X + + +
TRANSMISSION SIGNAL
RECEPTION CODE
X + X + + + X + X X
RECEPTION SIGNAL
RECEPTION DATA
1 0 1 1 0 1 0 0 0 1
COMMON KEY
SENDER
QUANTUM COMMUNICATION PATH
PUBLIC COMMUNICATION PATH
WIRETAPPER
RECEIVER